

Network Access Control (NAC)

Identity-based NAC with IPS and SIEM Integration



Complete solution featuring in-line and out-of-band appliances

Open, standards-based architecture and open APIs

Comprehensive dashboard reporting and advanced notification engine

Managed guest access control with sponsorship

Unified policy management in heterogeneous wired and wireless environments

Product Overview

Enterasys Network Access Control (NAC) is a complete standards-based, multi-vendor interoperable pre-connect and post-connect Network Access Control solution for wired and wireless LAN and VPN users. Using Enterasys **NAC Inline Controller** and/or **NAC Out-of-Band Gateway** appliances with **NMS NAC Manager** configuration and reporting software, IT administrators can deploy a leading-edge NAC solution to ensure only the right users have access to the right information from the right place at the right time. Enterasys NAC is tightly integrated with the Enterasys Intrusion Prevention System (IPS) and Enterasys Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control.

The Enterasys NAC advantage is business-oriented visibility and control over individual users and applications in multi-vendor infrastructures. NAC protects existing infrastructure investments since it does not require the deployment of new switching hardware or that agents be installed on all end systems. Enterasys NAC performs multi-user, multi-method authentication, vulnerability assessment and assisted remediation. It offers the flexibility to choose whether or not to restrict access for guests/contractors to public Internet services only—and how to handle authenticated internal users/devices that do not pass the security posture assessment.

Enterasys NAC policies permit, deny, prioritize, rate-limit, tag, re-direct, and audit network traffic based on user identity, time and location, device type, and other environmental variables. Enterasys NAC supports RFC 3580 port and VLAN-based quarantine for Enterasys and third-party switches, plus more powerful isolation policies (which prevent compromised endpoints from launching attacks while in the quarantine state) on Enterasys switches. Enterasys NAC is adaptable to any device using RADIUS for authorization with configurable RADIUS attributes such as Login-LAT or Filter ID. The solution offers unmatched interoperability, provides the widest number of authentication options, and supports Layer 2, Layer 3 and VPN access technologies.

Benefits

Business Alignment

- Protect corporate data by proactively preventing unauthorized users, compromised endpoints, and other vulnerable systems from network access
- Effectively balance security and availability for users, contractors and guests
- Proactively control the security posture of all devices on the network
- Efficiently address regulatory compliance requirements

Operational Efficiency

- Leverage existing assessment servers, authentication servers, software agents and identity sources avoiding forklift upgrades
- Gain IT efficiency
- Enable business staff to easily sponsor guests and validate guest registration

Security

- Enable the strongest security with fine grained access control based on user, device, time, location and authentication type
- Assess end systems of any type for vulnerabilities or threats with agent-based or agent-less assessment including third party tools
- Automate endpoint isolation, quarantine and remediation, plus ongoing threat analysis, prevention, and containment

Service and Support

- Industry-leading first call resolution rates and customer satisfaction rates
- Personalized services, including site surveys, network design, installation and training

There is nothing more important than our customers.

Enterasys NAC enables the homogeneous configuration of policies across multiple switch and wireless access point vendors. This capability significantly reduces the burden of policy lifecycle management and eases NAC deployment in wired and wireless heterogeneous infrastructures.

With Enterasys NAC's flexibility, organizations have phased deployment options enabling immediate network protection and business value. For example, an organization can start with simple endpoint detection and location directory information, then add authentication/authorization and/or assessment, and then automate remediation.

Fine-Grained Configuration Options

Enterasys NAC configuration options provide an unparalleled range of choices for fine grained network control. These configuration options include time, location, authentication types and end system and user groups. For example, enterprises can write and enforce policies that grant a precise level of network access based on the type of system connecting, an employee's role in the organization, the location of a user at the time the user is connecting, or the time of day. An enterprise's network is more secure with tighter control over who gains access, when and from what location. The granularity of these configuration options also provides flexibility for efficient deployment in large heterogeneous infrastructures.

Guest Account Services Included

Enterasys NAC includes automated guest registration access control features to assure secure guest networking without burdening IT staff. NAC capabilities automate or delegate guest access management. Features such as expiration and account validity time control the guest account without any IT involvement. Enterasys NAC provides a self registration portal for users to register multiple devices themselves. NAC offers advanced sponsorship capabilities such as email sponsorship and a simple portal for sponsors to use to validate guest registration. LDAP integration allows dynamic role assignment for authenticated registration. Authenticated registration allows enterprise network users to register devices and receive the proper role for non-802.1X capable devices. Multiple registration groups allow administrators to give different levels of access to different types of guests.

Identity-Aware Networking

In an identity-aware network a user's capabilities are controlled based on the user's identity and the access policies attributed to the user. Enterasys NAC provides user identity functionality including discovery, authentication and role based access controls. Enterasys NAC integrates with identity sources such as Siemens Enterprise Communications HiPath DirX Identity and Microsoft Active Directory leveraging and extending the organization's existing directory investments. Users are managed centrally in the identity system for the network and all connected applications. The process of managing the user's lifecycle (e.g. enrollment, role changes, termination) can be automated and linked to other business processes with LDAP and RADIUS integration. Users can be automatically added or deleted when they join or leave the organization. Enterasys identity-aware networking capabilities provide stronger network security and lower operational cost.

Endpoint Baselineing and Monitoring

All end systems in the network infrastructure should be incorporated in the network access control system for control to be most effective. Enterasys NAC provides agent-based or agent-less endpoint assessment capabilities to determine the security posture of connecting devices. Enterasys NAC, aligned with industry standards, works with multiple assessment servers, authentication servers and security software agents to match the needs of organizations who may have existing assessment technology. The agent-less capability does not require the installation of a software security agent on the end system and is typically used for end systems such as guest PCs, IP phones, IP cameras or printers. The Enterasys agent-less assessment scans for operating system and application vulnerabilities. The agent-based capability requires the installation of a software agent on the end system. The endpoint agent scans for anti-virus status, firewall status, operating system patches and peer-to-peer file sharing applications. The agent can look for any process or registry entry and automatically remediate. This combination of agent and agent-less capabilities in the Enterasys NAC solution enables more efficient management and reporting.

Notifications and Reporting

The advanced notification engine in Enterasys NAC provides comprehensive functionality and integrates with the workflows of other alerting tools already in place. Enterprises can leverage and extend their existing automated processes to further reduce operational costs. Notifications occur for end-system state changes, guest registration and end-system health results. Notification is delivered through traps, syslog, email or web service. The notification engine has the ability to run a program triggered by a notification event. For example, integrated with the help desk application, NAC notification can be used to automatically map changes in the infrastructure to actions.

End-system reporting is simple with Enterasys NAC web-based end-system data views. NAC provides easy-to-use dashboards and detailed views of the health of the end systems attached or trying to attach to the network. Analysts responsible for monitoring end-system compliance can easily tailor the views to present the information in their preferred format. The reports can be generated as PDF files.

NMS NAC Manager

NMS NAC Manager software provides secure, policy-based NAC management. From one centralized location, IT staff can configure and control the NAC solution, simplifying deployment and on-going administration. NAC Manager also aggregates network connectivity and vulnerability statistics and audits network access activities.

NMS NAC Manager provides additional value through its integration with other Enterasys NMS applications and Enterasys security products. For example, Enterasys NMS NAC Manager seamlessly integrates with NMS Policy Manager to enable "one click" enforcement of role-based access controls. The NMS NAC Manager IP-to-ID Mapping feature binds together the User, Hostname, IP address, MAC and location (switch and port or wireless AP and SSID) along with timestamps for each endpoint—a key requirement for auditing and forensics. IP-to-ID Mapping is also used by NMS Automated Security Manager to implement location-independent distributed intrusion prevention and by Enterasys Security Information and Event Manager (SIEM) or other third party SIEM/IPS solutions to pinpoint the source of a threat.

Enterasys NAC Inline Controller

The Enterasys NAC Inline Controller may be integrated into any network from any vendor to provide network access control for wired LAN, wireless LAN, and VPN users. The Enterasys NAC Inline Controller may be deployed without reconfiguration of network edge infrastructure. An in-line appliance, Enterasys NAC supports up to 2,000 endpoints and addresses a number of out-of-band NAC deployment challenges:

- Out-of-band NAC requires intelligent edge switches that support IEEE 802.1X authentication and RFC 3580 quarantine. Enterasys and some third party switches meet these requirements, but many older edge switches do not. The Enterasys NAC Inline Controller provides authentication and isolation for each user and application flow regardless of the edge switch deployed.
- Out-of-band NAC often requires reconfiguration of edge switches. The Enterasys NAC Inline Controller is installed in-line between the edge and distribution layers, and does not require any reconfiguration at the network edge.

Network performance and network fail-over availability are two important issues to consider when deploying any in-line security appliance. Because Enterasys NAC Inline Controllers take advantage of Enterasys advanced switch technology, these appliances will not become congestion points on the network. Dual Enterasys NAC Inline Controllers can be deployed in a fail-over mode where redundancy is required. Each communicates with the NMS NAC Manager application to replicate status and configuration information.

Assessment for the NAC Inline Controller is separately licensed and includes both agent-based and agent-less assessment.

Enterasys NAC Out-of-Band Gateway

The Enterasys NAC Out-of-Band Gateway controls endpoint authentication, security posture assessment and network authorization. For authentication services, the Enterasys NAC Out-of-Band Gateway acts as a RADIUS proxy, or RADIUS server for MAC Authentication, which communicates with the organization's RADIUS authentication services (e.g. interfaces with Microsoft Active Directory or another LDAP-based directory service). The Enterasys NAC Out-of-Band Gateway supports 802.1X (Extensible Authentication Protocol), MAC, Web-based and Kerberos Snooping (with certain restrictions) authentication. For endpoint assessment, the Enterasys NAC Out-of-Band Gateway connects to multiple security assessment servers.

For authorization services, the Enterasys NAC Out-of-Band Gateway communicates RADIUS attributes to the authenticating switch. This allows the switch to dynamically authorize and allocate network resources to the connecting endpoint based on authentication and assessment results.

The Enterasys NAC Out-of-Band Gateway appliance also stores NAC configuration information and the physical location of each endpoint. It easily scales to support redundancy and large NAC deployments. Enterasys NAC Out-of-Band Gateway models are available to meet the needs of different-sized implementations. It is also available as a security module for popular Enterasys switches.

Assessment for the NAC Out-of-Band Gateway is separately licensed and includes both agent-based and agent-less assessment.

Additional Features

- Proven interoperability with Microsoft NAP and Trusted Computing Group TNC.
- Automatic endpoint discovery and location tracking by identifying new MAC addresses, new IP addresses, new 802.1X / Web-based authentication sessions, or Kerberos or RADIUS request from access switches.
- Support for Layer 2 and Layer 3 deployment modes and support for all five NAC deployment models: intelligent wired edge, intelligent wireless edge, non-intelligent wired edge, non-intelligent wireless edge, and VPN.
- Management options (in-band or out-of-band) can be tailored to existing network management schemes and security requirements.
- Support for multiple RADIUS and LDAP server groups allows administrators to identify the server to which a request is directed.
- Macintosh agent support for agent-based assessment.
- Open XML API's support integration with IT workflows for automated streamlined operations
- Web-service based NAC API simplifies integration with third party applications.
- 1 + 1 Redundancy for both Layer 2 and Layer 3 deployment modes: provides high-availability and eliminates the NAC Inline Controller or NAC Out-of-Band Gateway as a single point of failure
- Risk level configuration allows flexibility in determining threat presented by the end system. Fine grained control allows NAC administrator to define High Risk, Medium Risk, and Low Risk thresholds based on local security policies and concerns.
- The Enterasys NAC Inline Controller and NAC Out-of-Band Gateway are upgradable, allowing assessment to be integrated onto a single box with the other NAC functions. The upgraded appliances are capable of supporting both network-based and/or agent-based assessment.

Specifications

Enterasys NAC Inline Controller

Physical Specifications

Form Factor: 19" rack mount; Height: 3.47" (8.81 cm); Width: 17.62" (44.46 cm); Depth: 20.44" (51.92 cm); Weight: 28 lbs (12.72 kg)

Power

Wattage: 400 watts maximum; Input Frequency: 50 to 60 Hz; Input Voltage: Range 2 x 100 to 125 VAC, 2X 200 to 240 VAC; Input Current: 120 V 3.6 Amps; 240 V 1.6 Amps

Environmental Specifications

Operating Temperature: 5° C to 40° C (41° F to 104° F); Storage Temperature: -30° C to 73° C (-22° F to 164° F); Operating Humidity: 5% to 90% RH, non-condensing

Agency and Regulatory Standard Specifications

Safety

UL 60950-1, FDA 21 CFR 1040.10 and 1040.11, CAN/CSA-C22.2 No. 60950-1, EN 60950-1, EN 60825-1, EN 60825-2, IEC 60950-1, 2006/95/EC (Low Voltage Directive)

Electromagnetic Compatibility

FCC 47 CFR Part 15 (Class A), ICES-003 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3, AS/NZS CISPR-22 (Class A), VCCI V-3, CNS 13438 (BSMI), 2004/108/EC (EMC Directive)

NMS NAC Manager

NMS NAC Manager is a plug-in application for the Enterasys Network Management Suite (NMS). NMS is available for 32-bit operating systems:

Windows (qualified on the English version of the operating systems)

Windows Server® 2003 w/ Service Pack 2
Windows XP® w/ Service Pack 2 or 3
Windows Vista® (Service Pack 1 Optional)
Windows Server® 2008 Enterprise
Windows Server® 2008 Enterprise 64-bit (as 32-bit application)

Linux

Red Hat Enterprise Linux WS and ES v4 and v5
SuSE Linux versions 10 and 11

Hardware Requirements

Recommended P4-2.4 GHz, 2GB RAM
(User's home directory requires 50MB for file storage)
(Windows Vista requires 2GB RAM)
Free Disk Space - 1GB

Remote Client

Recommended P4-2.4 GHz, 1GB RAM
(Windows Vista requires 2GB RAM)
Free Disk Space - 100MB
(User's home directory requires 50MB for file storage)
Supported Web Browsers:
Internet Explorer version 7 and 8
Mozilla Firefox 2.0 and 3.0
Java Runtime Environment (JRE) 1.5 or higher
(Windows Vista requires JRE 1.6 or higher)

Enterasys NAC Out-of-Band Gateway

Physical Specifications

NAC-A-20

Height: 1.68" (4.26 cm); Width: 18.99" (includes rack latches) (48.24 cm); Depth: 30.39" (includes PSU handles and bezel) (77.2 cm); Weight: 39 lbs (17.69 Kgs)

SNS-TAG-HPA and SNS-TAG-LPA

Form Factor: 19" rack mount; Height: 1.75" (44.4 mm); Width: 17.2" (437 mm); Depth: 17.8" (452.16 mm); Weight: 15.4 lbs (7 kg)

Power

NAC-A-20

Wattage: 717 Watt (high output), 570 Watt (Energy Smart); Voltage: 90- 264 VAC, autoranging, 47- 63Hz

SNS-TAG-HPA and SNS-TAG-LPA

Wattage: 400 watts maximum; Input Frequency 50 to 60 Hz; Input Voltage: Range 100 to 125 VAC; Input Current: 120 V 6 Amps; 240 V 3 Amps

Environmental Specifications

NAC-A-20

Operating Temperature: 10° to 35°C (50° to 95°F) with a maximum temperature gradation of 10°C per hour. Note: For altitudes above 2950 feet, the maximum operating temperature is de-rated 1°F/550 ft; Storage Temperature: -40° to 65°C (-40° to 149°F) with a maximum temperature gradation of 20°C per hour; Operating Humidity: 20% to 80% (non-condensing) with a maximum humidity gradation of 10% per hour

SNS-TAG-HPA and SNS-TAG-LPA

Operating Temperature: 5° C to 40° C (41° F to 104° F); Storage Temperature: -30° C to 73° C (-22° F to 164° F); Operating Humidity: 5% to 90% RH, non-condensing

Agency and Regulatory Standard Specifications

Safety

NAC-A-20

UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1, NOM

SNS-TAG-HPA and SNS-TAG-LPA

UL 60950, CSA C22.2 No. 60950, EN 60950, IEC 60950

Electromagnetic Compatibility

NAC-A-20

FCC Part 15 (Class A), ICES-003 (Class A), BSMI, KCC, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3

SNS-TAG-HPA and SNS-TAG-LPA

FCC: 47 CFR Parts 2 and 15, ICES-003, EN 55022, EN 61000-3-2, EN 61000-3-3, EN 55024, AS/NZS CISPR 22, VCCI V-3

NAC Assessment Agent OS Requirements

Supported operating systems for end systems connecting to the network through an Enterasys NAC deployment that is implementing Enterasys agent-based assessment.

- Windows 2000
- Windows 2003
- Windows 2008
- Windows XP
- Windows Vista
- Windows 7
- Mac OS X (Tiger, Leopard)

Certain assessment tests require the Windows Security Center which is only supported on Windows XP SP2+, Windows Vista, and Windows 7.

Ordering Information

NAC Inline Controller

Part Number	Description
2S4082-25-SYS	NAC Inline Controller, 24-Port Triple Speed, Uplink SFP, Optional Assessment
7S4280-19-SYS	NAC Inline Controller, 18-Port SFP, Uplink SFP, Optional Assessment

NMS NAC Manager

Part Number	Description
NS-NAC	NAC Manager (for use with existing NMS License)
NS-AB-50	NMS Advanced Bundle 50-devices (NMS Console with NMS NAC Manager, NMS Policy Manager, NMS Automated Security Manager, and NMS Inventory Manager)
NS-AB-U	NMS Advanced Bundle Unrestricted (NMS Console with NMS NAC Manager, NMS Policy Manager, NMS Automated Security Manager, and NMS Inventory Manager)

NAC Out-of-Band Gateway

Part Number	Description
NAC-A-20	Enterasys NAC Out-of-Band Gateway 3,000 endpoints, optional on-board assessment
SNS-TAG-HPA	Enterasys NAC Out-of-Band Gateway 3,000 endpoints
SNS-TAG-LPA	Enterasys NAC Out-of-Band Gateway 2,000 endpoints

NAC Assessment

Part Number	Description
NAC-ASSESS-LIC	Enterasys NAC Assessment, includes both agent-based and agent-less assessment

Transceivers

Enterasys transceivers provide connectivity options for Ethernet over twisted pair copper and fiber optic cables with transmission speeds from 100 Megabits per second to 10 Gigabits per second. All Enterasys transceivers meet the highest quality for extended life cycle and the best possible return on investment. For detailed specifications, compatibility and ordering information please go to: <http://www.enterasys.com/products/transceivers-ds.pdf>.

Warranty

As a customer-centric company, Enterasys is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Enterasys NAC comes with a one year warranty against manufacturing defects. Software warranties are ninety (90) days, and cover defects in media only. For full warranty terms and conditions please go to <http://www.enterasys.com/support/warranty.aspx>.

Service & Support

Enterasys Networks provides comprehensive service offerings that range from Professional Services to design deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Enterasys account executive for more information about Enterasys Service and Support.

Additional Information

For additional technical information on Enterasys NAC <http://www.enterasys.com/products/advanced-security-apps/enterasys-network-access.aspx>

Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at enterasys.com



© 2009 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

